Harlem Children's Zone
DATA PRIVACY AND SECURITY POLICY

To comply with applicable requirements of New York State Education Law §2-d and the accompanying the regulations (collectively, the "NYSED Data Privacy and Security Law"), Harlem Children's Zone (the "Organization") has adopted this Data Privacy and Security Policy (the "Policy").

Pursuant to the Policy:

- The Organization will designate a Data Protection Officer with responsibility for implementing the policies and procedures required by the NYSED Data Privacy and Security Law, and to serve as the point of contact for data privacy and security for the Organization.

- The Organization will not sell any personally identifiable information ("PII"), nor will it use or disclose it for any Commercial or Marketing Purpose or facilitate its use or disclosure by any other party for any Commercial or Marketing Purpose or permit another party to do so

- The Organization will take steps to minimize its collection, processing and transmission of PII.

- The Organization will ensure that it has provisions in its contracts with third-party contractors or in separate data sharing confidentiality agreements that require such third-party contractors to maintain the confidentiality of shared student, teacher, and/or principal data in accordance with federal and state law and the educational agency's data security and privacy policy.

- The Organization will publish on its website a parents bill of rights for data privacy and security (the "Bill of Rights") that complies with the provisions of NYSED Data Privacy and Security Law.

- The Organization will include the Bill of Rights in every contract the Organization enters into with a third-party contractor that receives PII, and will include supplemental information for each contract the Organization enters into with a third-party contractor pursuant to which that contractor receives student, teacher, or principal data. The Organization will develop this supplemental information and ensure it includes the requirements set forth in the NYSED Data Privacy and Security Law. Additionally, the Organization will publish on its website the supplement to the Bill of Rights for any contract or other written agreement with a third-party contractor that will receive PII.

- The Organization will establish and communicate to parents, eligible students, teachers, principals or other staff the Organization's procedure for filing complaints about breaches or unauthorized releases of student, teacher, or principal data.

- The Organization will safeguard data in accordance with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

- Every use and disclosure of PII by the Organization will benefit students and the Organization (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations).

- The Organization will not include PII in public reports or other documents.

- The Organization will ensure that it affords to parents or eligible students all applicable protections under FERPA and the Individuals with Disabilities Education Act (20 U.S.C. 1400 et seq.), as well as the accompanying regulations.

- The Organization will ensure that its contracts with third-party contractors include the third-party contractors' data security and privacy plan, which must be accepted by the Organization and must comply with the requirements set forth in the NYSED Data Privacy and Security Law.

- The Organization will annually provide data privacy and security awareness training to its officers and employees with access to PII. This training will include, but not be limited to, training on the state and federal laws that protect PII, and how employees can comply with such laws.

- If the Organization receives notification from a third-party contractor that the Organization's PII has been breached or subject to unauthorized release, the Organization will notify the New York State Education Department's Chief Privacy Officer within 10 calendar days following receipt of that notice.

- The Organization will report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the Chief Privacy Officer without unreasonable delay, but no later than 10 calendar days after such discovery or receipt of report.

- The Organization will also notify affected parents, eligible students, teachers and/or principals in the most expedient way possible and without unreasonable delay, but no later than 60 calendar days after the discovery of a breach or unauthorized release by the Organization or the receipt of a notification of a breach or unauthorized release from a third-party contractor unless that notification would interfere with an ongoing investigation by law enforcement or cause further disclosure of PII by disclosing an unfixed security vulnerability.

- The Organization will ensure that the notifications it provides in the event of a breach or unauthorized release are clear, concise, use language that is plain and easy to understand, and to the extent available, include: a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the Organization's investigation or plan to investigate; and contact information for representatives who can assist parents or eligible students that have additional questions.

- Parents and eligible students have the right to inspect and review a student's education record maintained by the Organization. All requests to inspect and review must be made by an individual or his or her representative in writing to the Organization in accordance with the Organization's access request procedure. The Organization will notify parents annually of their right to request to inspect and review their child's education record including any student data stored or maintained by the Organization.